ATTORNEY DOCKET NO.: ZIP00-01
SMALL ENTITY

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Robert D. Haskins and Dale P. Nielsen
Serial No.:	09/715,641
Title:	APPARATUS AND METHODS FOR CONTROLLING THE TRANSMISSION OF MESSAGES
Filing Date:	November 17, 2000
Examiner:	Jerry B. Dennison
Art Unit:	2143
Conf. No.:	7793

Certificate of Mailing Under 37 C.F.R. §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: **MAIL STOP APPEAL BRIEF PATENTS**, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

Date: February 9, 2006

By: Farah Z. Frasco
(Typed or printed name of person mailing Document, whose signature appears below)

Signature: _____

MAIL STOP APPEAL BRIEF PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Sir:

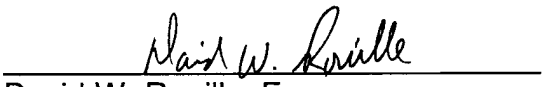
Enclosed is/are:

[x] Transmittal Letter (this form, 2 pages, in duplicate), Total Pages: 4;
[x] Supplemental Appeal Brief including Appendix (32 pages, in triplicate) Total Pages: 96;
[x] Return Receipt Pre-paid Postcard (in duplicate), Total postcards: 2;
[x] Authorization to charge Deposit Account No. 50-3735, if necessary.

Applicant hereby petitions for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Mail Room and/or the Application Branch is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,



David W. Rouille, Esq.
Attorney for Applicant
USPTO Registration No.: 40,150
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: ZIP00-01

Dated: February 9, 2006

Attorney Docket No.: ZIP00-01
SMALL ENTITY

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

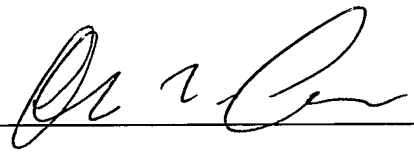
Applicants:	Robert D. Haskins and Dale P. Nielsen
Serial No.:	09/715,641
Filing Date:	November 17, 2000
For:	APPARATUS AND METHODS FOR CONTROLLING THE TRANSMISSION OF MESSAGES
Examiner:	Jerry B. Dennison
Art Unit:	2143
Conf. No.:	7793

Certificate of Mailing Under 37 C.F.R. §1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: **MAIL STOP APPEAL BRIEF PATENTS**, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

Date: February 9, 2006

By: Farah Z. Frasco
(Typed or printed name of person mailing Document, whose signature appears below)

Signature: 

MAIL STOP APPEAL BRIEF PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL APPEAL BRIEF

In response to Notice of Non-Compliant Appeal Brief of January 12, 2006, please consider this Supplemental Appeal Brief.

(1) Real party in interest.

Ziplink, a Delaware Corporation.

(2) Related appeals and interferences.

There are no related appeals or interferences.

(3) Status of claims.

Claims 1-28 stand rejected.

(4) Status of amendments

No amendment has been filed subsequent to the final rejection dated May 27, 2005.

(5) Summary of claimed subject matter

The present invention provides techniques and mechanisms that allow a computer system to control an amount of messages transmitted onto a computer network by an originator of the messages. By way of example, one embodiment of the system of the invention provides an e-mail quota enforcement system which prevents a sender of e-mail messages (e.g., a computer user) from sending a predetermined number of e-mail messages in a specific time interval that exceeds a quota assigned to the user for that interval. In this manner, a computer user is prevented from sending an unlimited number of e-mail messages onto a computer network such as the Internet. In other words, the system of the invention can be used to regulate "spam" sent by "spammers", which as explained above are the common terms for computer users (i.e., spammers) who send large volumes of e-mail messages (i.e. spam) to hundreds or thousands of individual recipients, many of whom often do not request such e-mail messages.

Figure 1 illustrates a computer system environment 100 configured in accordance with the invention. The computer system environment 100 includes a computer network 130 such as the Internet which interconnects an originator computer system 105 and a plurality of recipient computer systems 144-1 through 144-3. Certain groups of recipient computer systems such as 144-1 and 144-3 couple to the computer network 130 via respective destination message systems 140 and 142, while other recipient computer systems such as 144-2 may directly couple to the computer network 130. The destination message systems 140 and 142 may be, for example, recipient e-mail server systems

associated with network service providers that provide computer user accounts for the computer users of the recipient computer systems 144.

Disposed between the originator computer system 105 and the computer network 130 is a message quota system 120 configured according to embodiments of the invention to limit the number of outbound messages 110 that the originator computer system 105 can transmit onto the computer network 130 for receipt by the recipient computer systems 144. In a preferred embodiment of the invention, the outbound messages 110 are e-mail messages that the originator computer system 105 formats (e.g., addresses to recipients) and transfers according to an e-mail transfer protocol such as the Simple Mail Transfer Protocol (SMTP) onto the computer network 130.

Figure 2 illustrates the general processing steps 250 through 254 that the message quota system 120 performs according to embodiments of the invention to limit the transmission of outbound messages 110 onto the computer network 130. The high-level operation of the message quota system 120 shown in Figure 1 will be explained with respect to the processing steps in Figure 2.

In operation of the system of the invention, the originator computer system 105 transmits one or more outbound messages 110 for receipt by certain of the recipient computer systems 144 via transmission through the computer network 130. In step 250, the message quota system 120 detects the outbound message 110 (e.g., via receiving such a message) from the originator, which in this case is the computer user controlling the originator computer system 105.

In step 251, the message quota system 120 performs a quota enforcement operation (e.g., via software control, not specifically shown) based on a message count and a message limit, both of which are associated with the computer user controlling the originating computer system 105, to produce a message transmission result. That is, the message quota system 120 maintains a message count associated with the originator identity (e.g., a computer user account name) of the originator who transmitted the outbound message 110 that indicates how many messages have been sent using the originator identity over a certain prior period of time. The message quota system 120 also maintains at least one message limit associated with the originator identity that indicates a maximum number of messages that are allowed to be transmitted onto the computer network 130 for that particular originator identity over a specific interval of time. Generally, the message count(s) corresponds to the message limit(s) in that respective message counts are compared to respective message limits, as will be explained. Based on the message count and the message limit associated with the originator identity obtained foreign outbound message 110, the quota enforcement operation can determine the message transmission result that indicates whether or not the outbound message 110 should be transmitted onto the computer network 130.

Next, in step 252, the message quota system 120 performs a selective transmit operation that transmits (e.g., propagates onto the computer network 130) the outbound message 110 from the originator computer system 105 onto the computer network 130 if the message transmission result, as determined by the quota enforcement operation, contains a "transmit" value (sub-step 253) . Alternatively, the message quota system 120 prevents transmission of the outbound message 110 from the originator computer system 105 onto the computer network 130 if the message transmission result produced as a result of the quota enforcement operation (step 251) contains a "no-transmit" value (sub-step 254).

In this manner, the system of the invention prevents, for example, a user of the originator computer system 105 from transmitting an unlimited number of outbound messages 110 onto the computer network 130 destined for an unlimited number of recipients 144. In the case of e-mail messages, the system of the invention thus prevents a person from "spamming" recipients with bulk or unwanted e-mail messages. In doing so, the computer network such as the Internet is not subject to abusive spam email messages from computer user who have accounts (i.e., subscribe to network service) with a network service provider that uses the system of the invention. Accordingly, since message use is limit to required use (as imposed by a proper setting of the message limits for a particular originator identity), and not spam or junk message use, the domain associated with the network service provider is somewhat protected from being labeled as a "source of spam" on the computer network. In other words, conventional network service providers can become known sources of spam over time and thus computer users on the Internet might tend to configure their browsers to reject messages from domains associated with those network service providers. However, using the invention, a network service provider can protect itself from becoming labeled in this manner since the invention limits the amount of message a user can send from his or her network service provider. As such, chances are greater that a particular user will use his or her message limit to send legitimate messages instead of junk or spam related messages.

Since the system of the invention enforces a message quota within the sending transmission path that an outbound message 110 must initially traverse from an originator computer system 105, onto the computer network 130, to a destination recipient 144, the system of the invention limits outbound message traffic from the originator computer system 105 to a number of outbound messages 110 allowed by the quota for the particular computer user who transmits such outbound messages 110.

Furthermore, since the system of the invention performs outbound message quota enforcement prior to the outbound messages 110 leaving the domain or realm of a network service provider (not specifically shown in figure 1) that provides a computer user account for the computer user

controlling the originator computer system 105, unsolicited or unwanted outbound messages 110 (e.g., spam) are curtailed prior to reaching a computer network 130 thus saving computer network resources. As noted above, the domain or realm of the network service provider that uses the message quota system 120 of the invention will not be perceived by users of recipient computer systems 144 as being a producer of such unsolicited or unwanted outbound messages 110. The invention also results in recipient computer users not having to manually configure e-mail client software programs to reject unsolicited e-mail. Nor are such users required to delete such unsolicited e-mail because the system of the invention prevents the originator computer system 105 from transmitting unsolicited e-mail in the first place.

Figure 3 illustrates a more detailed architecture of the message quota system 120 configured according to one embodiment of the invention and also illustrates a bit more detail concerning the content of an outbound message 110, which is an e-mail message in this example. The message quota system 120 generally includes connection equipment 148 which couples to a quota server 160. The quota server 160 in this example embodiment is a Simple Mail Transfer Protocol (SMTP) server modified according to embodiments of the invention. The message quota system 120 also includes a login database 156, a quota database 162, and optionally a domain name service 164. The connection equipment 148 comprises a remote access server 150 coupled to a port redirector 158 and an authentication server 152, which includes a login extractor process 154. The operation of these components will be explained with respect to Figure 4.

Figure 4 provides a flow chart of processing steps that the connection equipment components within the message quota system 120 perform according to embodiments of the invention. Generally, the connection equipment 148 receives and authenticates connections 166 on behalf of computer user accounts operated by computer users controlling the originator computer system(s) 105 (only one shown in this example). Once a computer user has established a connection 166 with the connection equipment 148, during the remainder of the duration of the connection 166 (i.e., during the duration of the data communications session 166 between the originator computer system 105 and the message quota system 130) the connection equipment 148 is responsible for directing outbound messages 110 that are to be subject to the quota enforcement system of the invention to the quota server 160 for processing as explained below.

More specifically, with respect to the flow chart in Figure 4, in step 400, the remote access server 150 operates in conjunction with the authentication server 152 to allow a computer user controlling the originator computer system 105 to connect 166 to the remote access server 150. The remote access server 150 may be, for example, dial-in network access server equipment such as a modem

bank that allows computer users of computer systems such as the originator computer system 105 to dial-in to computer user accounts provided by a network service provider for access to the computer network 130.

The authentication server 152 in this example embodiment is a RADIUS (Remote Authentication Dial-in User Services) server which executes or otherwise performs RADIUS authentication and accounting software functions according to techniques defined by Request For Comments 2138 and 2139 (RFC2138 and RFC 2139), the contents and teachings of which are hereby incorporated by reference in their entirety. Generally, when a user of the originator computer system 105 dials-in or otherwise connects to the remote access server 150, the remote access server 150 interacts 170 with the authentication server 152 (e.g., via RADIUS authentication and authorization techniques) to authenticate and authorize access to a computer user account provided by the remote access server 150 for the computer user operating the originator computer system 105.

In the example in Figure 3, the authentication server 152 authenticates the computer user designated by the account name JOE@XYZ.COM. Thus, user JOE@XYZ.COM logs in to the remote access server 150 (step 400, Figure 4) and the remote access server 150 dynamically assigns the network IP address 206.15.168.1 to the originator computer system 105. During establishment of the connection 166, the remote access server 150 may assign the network address (IP address 206.15.168.1 in this example) via a dynamic address assignment mechanism such as the Dynamic Host Configuration Protocol (DHCP) that operates between the remote access server 150 and the originator computer system 105 during the login and authentication process of step 400.

Next, in step 401, the login extractor 154 configured according to embodiments of the invention extracts login information (not specifically shown) from the authentication server 152 into the login database 156 by creating a mapping of the originator address (e.g., the network IP address) which the remote access server 150 assigned to the originator computer system 105 during connection setup (step 400) to an originator identity (i.e., the user account JOE@XYX.COM) of the computer user operating the data communications session 166. In a preferred embodiment, the login extractor 154 is a computer program that operates on the authentication server 152 to continuously monitor login information (e.g., RADIUS accounting data, not specifically shown) that the authentication server 152 (i.e., RADUIS software) produces in response to each instance of a computer user operating the originator computer system 105 to connect 166 to the remote access server 150 (i.e., in step 400) via a user account.

Figure 5 illustrates an example of the content which the login extractor 154 writes to the login database 156 in step 401. In this embodiment, each entry (e.g., a row, only one shown in this

example) in the login database 156 includes an originator identity 212 (e.g., a user account name) mapped to a respective originator address 204 along with a corresponding session start time 206. Essentially, the login extractor 154 maintains a mapping between currently active user account names and respective network addresses in use by those user account names. The session start time 206 indicates the time at which the user account associated with the originator identity 212 established the connection 166 with the remote access server 150. With respect to the specific illustrated example in Figure 3 and the example entry in the login database 156 in Figure 5, the login database entry indicates that the originator identity JOE@XYZ.COM is currently using an originator network address of 206.15.168.1 and commenced the connection 166 at 6:48 PM. Once the login extractor 154 has performed step 401, the system of the invention is relatively passive until the computer user (e.g., JOE@XYZ.COM) attempts to send an outbound message 110. If the user logs out or disconnects, thus breaking the connection 166, the login extractor 154 can also detect this condition and then removes the entry (i.e., the row) in the login database 156 that mapped that user's originator identity to that originator address 204.

Returning attention now to the processing steps in Figure 4 and the example embodiment in Figure 3, assume for this example that the computer user operating under the account name JOE@XYZ.COM attempts to send the example outbound e-mail message 110 shown in Figure 3 from the originator computer system 105 to the computer network 130 (Figure 1).

The port redirector 158 detects this action in step 402. For example, in step 402, the port redirector 158 can detect the outbound message 110 from the originator (e.g., computer user JOE@XYZ.COM) upon its transmission for the originator computer system 105 via connection 166 to the remote access server 150. In a preferred embodiment of the invention, the port redirector 158 is a "Layer 4" data communications switch which is capable of detecting content of such as protocol information or other packet information within the outbound message 110 and is capable of switching the outbound message 110 to alternate destinations based upon such content.

Next, in step 403, the port redirector 158 determines if the outbound message 110 contains content that indicates that the outbound message 110 should be subject to the message quota enforcement system of the present invention. If the port redirector 158, in step 403, determines that the outbound message 110 is to be subject to the message quota enforcement techniques of the invention (as will be explained), the port redirector 158 redirects the outbound message 110 on data communications path 175 to the quota server 160 to perform the message quota enforcement processing. The message quota enforcement processing is shown by processing steps in Figure 7, which will be explained shortly. However, if in step 403, the port redirector 158 determines that the outbound message 110 is

not subject to the message quota enforcement techniques of the invention (discussed below), the port redirector 158 redirects the outbound message 110 on data communications path 178 to a message server program 180, such as an e-mail server program in this example, for propagation onto the computer network 130 to one or more recipients to the outbound message 110.

In one embodiment of the invention, all outbound messages 110 are subject to message quota enforcement according to the techniques explained herein. By way of example, the port redirector 158 can redirect all outbound messages 110 (e.g., packets of data containing e-mail messages) that are directed to the Transmission Control Protocol (TCP) port twenty five (25), which is the TCP protocol port used to transmit e-mail messages on a data communications network.

Alternatively, depending upon the configuration of the invention, it may be the case, for example, that only certain computer user accounts (i.e., originator identities) or certain designated originator addresses, domain names, realms, etc., from which outbound messages 110 originate, are to be subject to the quota enforcement techniques of the invention. Accordingly, step 403 provides the ability for the port redirector 158 to determine whether or not each outbound message 110 is to be processed according to the quota enforcement techniques of the invention or not based on content contained within that outbound message 110. That is why in this example the port redirector 158 is a Layer 4 switch which is capable of analyzing protocol and/or data content contained within an outbound message 110.

As shown in Figure 4, the port redirector generally repeats processing steps 402, 403 and 404 or 405 for each outbound message 110 that the port redirector 158 detects during the duration of the data communications session 166. That is, once the computer user JOE@XYZ.COM has established the connection 166 with the remote access server 150 via steps 400 and 401, during the duration of this connection 166, the port redirector 158 will detect (Step 402) and forward or redirect (step 403 and 404) all outbound messages 110 which are subject to message quota enforcement to the quota server 160 and will forward (step 403 and 405) all other outbound messages 110 (i.e., those not subject to message quota enforcement) to a message server 180 for further processing on the computer network 130. That is, once the connection equipment 148 has completed the process of establishing the connection 166 and begins receiving outbound messages 110 from the originator computer system 105, as explained above, the port redirector 158 redirects such outbound messages 110 to the quota server 160 for quota enforcement processing.

Prior to explaining the details of the operation of the quota server 160, attention is directed now to the example outbound message 110 illustrated in Figure 3. In this example, the outbound message 110 is an e-mail message containing various content fields 190 through 194. In particular, the

outbound e-mail message 110 includes a source or originator address field 190 which contains the originator network address 206.15.168.1. This is a network address that the remote access server 150 assigns to the originator computer system 105 during the establishment of connection 166. Note that this network address field 190 may change in value each time the computer user controlling the originator computer system 105 re-establishes a new connection 166 with a remote access server 150. However, for any number of outbound messages 110 transmitted from the originator computer system 105 using a particular connection 166, the value of the originator address field 190 remains the same and is equivalent to the network address assigned to that connection 166 for the originator computer system 105.

The outbound message 110 also includes an account name field 190 which in this example is the "FROM:" field of the e-mail message that contains the account name JOE@XYZ.COM. As mentioned above, sophisticated computer users can manipulate email software client programs (not specifically shown) on the originator computer system 105 to produce a fraudulent value for the account name field 192 within an outbound e-mail message 110. Accordingly, in the case of spam or unsolicited outbound e-mail messages 110, it is often the case that the value in the account name field 192 is different from the actual originator identity 212 provided during the establishment of the connection 166. Stated differently, the login extractor 154, as explained above, obtains the true originator identity 212 (Figure 5) and currently assigned originator network address 204 (Figure 5) of the computer user operating the originator computer system 105 during the authentication process (steps 400, 401 in Figure 4) required to establish the connection 166. However, once this computer user has established the connection 166, any outbound messages 110 sent by that computer user may contain a fraudulent account name field 192 that does not match the originator identity 212 stored within the login database 156.

The outbound e-mail message 110 also contains a plurality of recipient fields 192 respectively labeled "TO:" "CC:" and "BCC:" that in this example each contain a list of recipient e-mail addresses (e.g., USERS 1..Q@ABC.COM, USER1..R@DEF.COM, and USERS1..S@HIG.COM) corresponding to various recipient computer users 144 (Figure 1) on the computer network 130. One objective of the present invention is to limit the amount of recipients 192 that can receive a particular outbound message 110.

As explained above in the background of the invention, a problem exists in conventional e-mail systems in that a computer user controlling an originator computer system 105 can essentially designate an unlimited number of recipients 192 for an outbound message 110 which causes significant processing burdens on hardware and software within the computer network 130.

Furthermore, also as explained above, a computer user can attempt to fraudulently identify the account name value in the account name field 192 of an e-mail address 110 such that recipient computer users 192 will be unable to easily detect the true originator identity 212 of the sender of the outbound message 110. The quota enforcement system of the invention is able to curtail such abuses of e-mail transmissions by limiting the number of recipients 192 of outbound messages to a particular amount over a certain time interval for a particular user account associated with the true originator identity 212 of the computer user sending outbound messages 110. In other words, if a computer user generates an outbound message 110 with a large amount of recipients 192 (or generates many outbound message with a large or small number or recipients 192 in each message 110) and possibly attempts to fraudulently modify the account name field 192, the system of the invention is still able to enforce message quotas is based on the true originator identity 212 that the computer user must provide during the establishment of the connection 166.

Figure 7 shows an example of message quota enforcement processing steps in accordance with one embodiment of the invention. Generally, a processor (not specifically shown) within the quota server 160 performs the message quota processing steps shown in Figure 7 to determine whether or not an outbound message 110 should be transmitted to its intended recipient(s) 192 on the computer network 130.

In step 500, the quota server 160 receives an outbound message 110 that is to be subject to the message quota enforcement processing explained herein. As explained above, outbound messages 110 that the quota server 160 receives are generally forwarded to the quota server 160 via the port redirector 158. In a preferred embodiment of the invention, the quota server 160 is a modified version of a mail server program such as the Simple Mail Transfer Protocol Demon (SMTPD) server program. The modifications to the SMTPD program include adding the quota enforcement functionality explained herein.

Next, in step 501 the quota server 160 obtains the originator address 190 within the outbound message 110. As indicated above, this originator address 190 remains constant for the duration of the connection 166 with the remote access server 150.

Next, in step 502, the quota server 160 obtains the originator identity 212 associated with the originator address 190 from the login database 156. As an example, the quota server 160 can query the login database 156 based on the originator address 190 to obtain the originator identity 212 that indicates which computer user the originator computer system 105 is using to transmit the outbound message 110. Recall from the processing of the connection equipment 148 as explained above, the login extractor 154 produces a mapping in the login database 156 between the true originator identity

212 of the account name used to establish the connection 166 and the originator network address 204 that is currently assigned to the connection 166. Accordingly, the originator identity 212 obtained in step 502 from the login database 156 is the true originator identity 212 associated with the account name that is being used in an attempt to transmit the outbound message 110 from the originator computer system 105.

Now that the processing of the invention has determined the true originator identity 212 (i.e., has determined which Internet network service provider user access account) that the originator computer system 105 is using to attempt to transmit the outbound message 110, the system of the invention can determine one or more current message counts associated with that originator identity. Generally, as used herein, the term "message count" refers to a current number of messages that have been sent during a predetermined time interval, where each recipient of an outbound message 110 counts as one message count.

Accordingly, in step 503, the quota server 160 obtains (e.g., via a query), from the quota database 162, the current set of one or more message counts 214 for the originator identity 212 determined in step 502. The current set of one or more message counts 214 for the originator identity 212 indicate how many messages (one per recipient) have been sent using the account name of the originator identity 212 over an elapsed predetermined amount of time.

Figure 6 illustrates a specific example of the content of the quota database 162. Each entry (i.e., each row, only one shown in this example) in the quota database 162 indicates the current message counts 214 and message limits 216 for a particular originator identity 212. In the instant example, the originator identity 212 JOE@XYZ.COM has two associated message counts 214. Example message count 214-1 indicates that the user account having the originator identity 212 of JOE@XYZ.COM has previously transmitted eighty four (84) messages within the past twenty four (24) hours. Likewise, message count 214-2 indicates that this same user account has transmitted twenty four (24) messages in the past five (5) minutes of elapsed time, as measured by the quota server 160. Again, it is to be understood that for the purposes of this explanation, each recipient of a message counts as one message.

Referring now to the example message limits 216 for the originator identity 212 JOE@XYZ.COM in the quota database 162, the message limit 216-1 indicates that this user account is allowed to (i.e., is restricted to) transmit one hundred (100) outbound messages 110 within a given twenty four (24) hour time interval (e.g., as measured by the quota server 160 for the most recent 24 hours that have elapsed), while message limit 216-2 indicates that this user account is allowed to transmit twenty five (25) outbound messages 110 within any given five (5) minute time interval of elapsed time. The

message limits 216 thus define the maximum quotas of outbound messages 110 that a particular account name associated with the originator identity 212 can transmit over a predetermined time interval as specified in the message limits 216. Generally, in this embodiment, message count 214-1 corresponds to message limit 216-1, while message count 214-2 corresponds to message limit 216-2. That is, as will be explained next, message count 214-1 is compared with message limit 216-1 to determine if the message limit 216-1 has been exceeded, while message count 214-2 is compared with message limit 216-2, and so forth.

It is to be understood that these message counts and message limits are provided as examples only and are meant to illustrate the concepts of the invention. It is also meant to be understood that while the present example illustrates two message counts 214 corresponding to two message limits 216 for a particular originator identity 212, there can be any number (zero or more) of message limits 214 and associated message counts 216 assigned to a particular originator identity 212.

Returning attention now to the processing in Figure 7, the quota server 160 can perform step 503 to obtain the current message counts 214 for the particular originator identity 212 obtained in the processing of step 502 via a query to the quota database 162.

Next, in step 504, the quota server 160 obtains (e.g., via a query) the message limits 216 from the quota database 162 based on the originator identity 212 as obtained in step 502.

At this point, the message quota processing of the invention can make the determination of whether or not the outbound message 110 is allowed to be transmitted or not onto the computer network 130 to one or more of the recipients 192. Generally, this is done by comparing the current message counts 214 against a corresponding message limits 216 to determine if any of the message counts 214 exceed the message limits 216.

In particular, in step 505, the quota server 160 determines if any message counts 214 exceed their corresponding message limits 216. If the quota server 160 determines in step 505 that any message count 214 exceeds its corresponding message limit 216, then processing proceeds to step 412 where the quota server 160 prevents further transmission of the outbound message 110 to any recipients 192 by setting a message transmission result (not specifically shown) to a "NO-TRANSMIT" value and reports this condition to a log file (not specifically shown). While not shown in the figures, at this point (step 505), the quota server 160 can return a "QUOTA EXCEEDED" message back to the originator computer system 105 based on the originator identity 212. Such a "QUOTA EXCEEDED" message might, for example, indicate to the computer user controlling the originator computer system 105 what his or her message limits 216 are and how long that computer user will have to wait before

being able to transmit an outbound message using the account name associated with the originator identity 212.

Alternatively, in step 505, if the quota server 160 determines that no message counts 214 currently exceed their corresponding message limits 216 for the originator identity 212, than processing proceeds to step 507.

In step 507, the quota server 160 updates the appropriate message counts 214 associated with the originator identity 212. In particular, in a preferred embodiment, each message count 214-1 and 214-2 are incremented by the number of different recipient identities listed in all of the "TO:" "CC:" and "BCC:" recipient fields 192 within the outbound message 110. In this manner, the current message counts 214 for the originator identity 212 of the account sending the outbound message 110 are updated to take into account recipients 192 of the outbound message 110. For example, if there are ten (10) different recipients designated in the recipient field 192 in the outbound message 110, then the quota server can increment each of the message counts 214-01 and 214-2 by ten (10).

It is understood that variations of this particular embodiment are possible while still remaining within the scope of the invention. For example, prior to performing step 507, the example message count 214-2 illustrated in Figure 6 indicates that twenty four (24) messages have been sent in the past five (5) minutes by JOE@XYZ.COM (i.e., originator identity 212). However, the message limit 216-2 indicates that JOE@XYZ.COM is only allowed to send twenty five (25) messages 110 in a five minute interval. Accordingly, in one alternative embodiment, if the current outbound message 110 discussed in the above example contains ten (10) recipients, when the quota server 160 performs step 507 to update the message counts 214 for the originator identity 212 (JOE@XYZ.COM in this example), the message count 214-2 might be incremented to 34. This value would clearly be in excess of the message limit 216-2.

One embodiment of the invention provides a solution to this dilemma by having the quota server 160, in the update message count processing in step 507, compute the difference between the corresponding message limits 216 and the current message counts 214 (e.g., message limit 216-2 minus (-) message count 214-2 = 1, in this example). The result indicates how many copies of the outbound message 110 can be transmitted at the current time. In the instant example, only one copy of the message 110 can be sent at this time since the difference between the message limit 216-2 and message count 214-2 is one. The one copy of the outbound message 110 would be sent in this case to the first recipient listed in the recipient list 192 for that message 110. The quota server 160, in this embodiment, can then buffer the remaining copies of the outbound message 110 (one copy per each recipient designated in recipient field 192) for transmission at a later time, when the message counts

214 for their associated time intervals have been reduced, as explained below. Alternatively, the quota server 160 can discard any messages 110 for recipients 192 beyond the difference between message limit 216-2 and message count 214-2. In this manner, the system of the invention is able to limit the number of recipients 192 that can receive an outbound message 110 by one ore more message limits 216.

In other words, in one embodiment of the invention, if a message count 214 has only X remaining messages that can be sent before that count exceeds its corresponding limit 216, then the invention in steps 505 and 507 will only allow X recipients to receive that message and will not allow the remaining recipients to get a copy of the message 110.

While not specifically shown as data within the quota database 162, the quota server 160 can determine and maintain an elapsed session time by comparing the current time with the session start time 214 obtained by the login extractor 154 within the login database 156. Such as elapsed session time value can be used to further update the message counts in step 507 by lowering or reducing the value of the message counts 214 for a particular originator identity 212 in the event that the elapsed time for a particular message count 214 has exceeded the time designated in a corresponding message limit 216 for that message count 214. The quota server 160 can perform such a reduction in message counts 214 over a sliding window or interval of time. In other words, since the quota server 160 is aware of the start time of the data communications session 166, and is further aware of each time (e.g., via a timestamp, not shown) at which each outbound message 110 is attempted to be transmitted onto the computer network 130 (e.g., the quota server 160 can maintain a timestamp record of the time at which each outbound message 110 is provided with a message transmission result having a "TRANSMIT" value, as will be explained shortly), the quota server 160 can use known processing techniques (e.g., simple measurements over time) to determine exactly how many outbound messages 110 have been transmitted in the most recent window of time designated by the time interval specified by each message limit 216-1 and 216-2. As this window of time progresses and no further message are sent, the message counts can be lowered.

In this manner, while receipt and transmission of outbound messages 110 to each recipient 192 results in the message counts 214-1 and 214-2 each being incremented by a value of one (1) for each recipient, concurrently with this process, as sufficient amounts of time elapse, the quota server 160 also can perform a process of decrementing the message counts 214 accordingly to credit the originator identity 212 with the ability to send more message 110 as periods of time elapse during which the originator identity 212 attempts to transmits no messages 110. The quota server 160

performs such incrementation and decrementation of the message counts 214 (i.e., updating of message counts) in step 507.

Upon completion of step 507, the quota server 160 performs step 508 to allow transmission of any copies of the outbound message 110 (one per designated recipient 192) that are within the message limits 214, as explained above, by setting a message transmission result to a "TRANSMIT" value for each recipient copy of such outbound messages 110.

After the quota server 160 performs either step 506 or step 508, the quota server 160 performs step 509 to process a copy of the outbound message 110 for each recipient 192 based on the message transmission result. In other words, step 509 is equivalent to step 252 in Figure 2 which performs a selective transmit operation based on the message transmission result. For copies of the outbound message having a "TRANSMIT" value as their message transmission result, the quota server will forward such messages 110 on to a secondary message server 180. As indicated above, the quota server 160 will either reject or discard any outbound messages 110 that contain a "NO-TRANSMIT" value as their message transmission result.

In this manner, the system of the invention is able to control transmission of outbound messages 110 transmitted from originator computer systems 105 for receipt by recipients on the computer network 130. The system of the invention is extremely beneficial in situations where a computer user attempts various techniques for spoofing an e-mail server program into transmitting large amounts of unsolicited bulk outbound messages 110. For example, since the system of the invention tracks message quotas at the user account level (i.e., based upon unique originator identities 221 for a user account provided by a network service provider), it makes no difference how many times a computer user connects, transmits outbound messages, disconnects, and then reconnects again in an attempt to circumvent the system of the invention. Even though the originator computer system 105 obtains a unique and different network address (i.e., originator address 204) each time the computer user establishes a new connection 166, since the system of the invention maps these network originator addresses 204 back to the true originator identity 212 of the user account that the computer user uses to transmit outbound messages 110, the message counts 214 associated with that originator identity 212 are accurately maintained by the system of the invention. Accordingly, unless the computer user has access to an unlimited number of user accounts (a highly unlikely situation), once the user account assigned to a particular computer user reaches its message limit 216 for the predetermined time interval for that message limit 216, that computer user is prevented from further transmitting outbound messages 110.

Figure 8 illustrates an alternative example a computer system environment 101 configured according to embodiments of the invention. The computing system environment 101 includes two network service providers 182 and 183. The network service provider 182 includes the connection equipment 148 configured in accordance with the invention, as previously explained. The network service provider 182 also includes a message server 184. The network service provider 183 is equipped with a quota server 160 configured to operate according to embodiments of the invention, also as previously explained. Accordingly, the network service provider 183 offers a quota enforcement service that other network service providers can subscribe to, as does the network service provider 182 in this example.

In this example, suppose the network service provider 182 subscribes to a message quota enforcement service offered by the network service provider 183. As such, upon subscription to such a quota enforcement service, technicians (i.e., people such as systems administrators) associated with the network service provider 182 install the port redirector 158 (Figure 3, if a port redirector does not currently exist) and login extractor 154 process within the connection equipment 148 at the facilities of the network service provider 182. Once the network service provider 182 has connection equipment 148 configured to operate as explained above, the connection equipment 148 performs the operations shown in Figure 4.

In other words, the connection equipment 148 authorizes and authenticates connections 166 to the computer network 130 from originator computer systems 105 (e.g., via step 400). The login extractor 154 within the connection equipment 148 operates to capture, in the login database 156, a mapping between an originator identity 212 (Figure 5) and a corresponding originator address 204 (Figure 5) for the connection 166 (e.g., via step 401). Finally, the port redirector 158 detects (step 402) and redirects (steps 403 and 404) all outbound messages 110 (to which quota enforcement is to be applied) via data communications path 175 through the computer network 130 to the quota server 160 that operates within the domain or realm of the network service provider 149. In this manner, the network service provider 182 does not need to contain, maintain or operate the quota server 160.

Once the quota server 160 operating within the realm of the network service provider 183 receives, via data communications path 175, the redirected outbound message(s) 110, the quota server 160 within the network service provider 183 operates according to the processing shown in Figure 7 to accept or deny the transmission of the outbound message(s) 110 for each recipient (e.g., recipients 192 in Figure 3) designated in that message 110. For those outbound messages 110 which the quota server 160 determines should be allowed for transmission on the computer network 130 (i.e., for those messages 110 for recipients which do not exceed the quota or message limit 216 for a particular

originator identity 212), the quota server 160 forwards those outbound messages 110, via data communications link 177, to the message server 184 within the network service provider 182. The message server 184 is the email server for network service provider 184 which then propagates each message to its intended recipient.

In this manner, the embodiment of the invention illustrated in Figure 8 divides portions of the invention between different network service providers 182 and 183. Network service provider 183 can operate as a quota enforcement clearinghouse that provides a message quota enforcement subscription service to other network service providers that do not have such capabilities themselves. As explained above, for this to occur, the network service providers (e.g., 182) that desire to subscribe to such a service are properly configured to redirect all outbound messages 110 (e.g., via a Layer 4 switch or via another means such as a content router) which are to be subject to the message quota subscription enforcement service to the quota server 160 operating within the realm of the network service provider 183. Also, network service providers that subscribe to such a service are equipped with the login extractor 154 in order to determine the true originator identity 212 of computer user accounts which generate outbound messages 110 for propagation onto the computer network 130.

(6) Grounds of rejection to be reviewed on appeal.

Whether Claims 1-28 are unpatentable over Tello et al. (U. S. Patent No. 6,381,634) in view of Janacek et al. (U.S. Patent No. 6,684,248) under 35 U. S. C. §103(a) and further as being unpatentable over Tello in view of Barchi (U.S. Patent No. 6,507,866).

(7) Argument.

Claims 1-28 stand rejected under 35 U.S.C. §103 (a) as being unpatentable over Tello et al. (U. S. Patent No. 6,381,634) in view of Janacek et al. (U.S. Patent No. 6,684,248). Claims 1-28 also stand rejected under 35 U.S.C. §103 (a) as being unpatentable over Tello et al. (U. S. Patent No. 6,381,634) in view of Barchi (U.S. Patent No. 6,507,866).

I. The Examiner's Position

The Examiner's rejection is presented below:

In the first Office Action dated December 2, 2004, the Examiner stated the following:

> Claims 1, 2, 12-14, 15, and 26-28 are anticipated by Tello which discloses at column 5, lines 45-65 and column 6, lines 9-20 an SCP server

detecting outbound messages from subscribed users, and performing a quota enforcement operation by comparing the number of messages sent by a user with a global threshold limit. If the message count exceeds the threshold limit, the messages do not get transmitted, and an error message is returned.

However Tello does not explicitly state when the result is a transmit value, updating a message count associated with the originator identity of the outbound message. Janacek discloses a method of transferring data from a sender to a recipient including a server that contains a database that keeps track of user statistics, including a message count which tracks the total number of messages sent by the user.

The Examiner further stated that claims 1-6, 12, 14-17, and 26-28 are anticipated by Tello which discloses at column 5, lines 45-65 and column 6, lines 9-20 an SCP server detecting outbound messages from subscribed users, and performing a quota enforcement operation by comparing the number of messages sent by a user with a global threshold limit. If the message count exceeds the threshold limit, the messages do not get transmitted, and an error message is returned. In regards to verifying an authenticity of an originator address associated with the outbound message, Tello discloses password protected accounts for users to use their unique email addresses.

However Tello does not explicitly state when the result is a transmit value, updating a message count associated with the originator identity of the outbound message. Barchi discloses an email usage pattern detection system that checks whether the number of email messages from a single originator has exceeded predetermined thresholds at column 7, line 65 through column 8, line 10.

In the final Office Action dated May 27, 2005, the Examiner repeated the objection given in the first office action.

Response to Arguments

Applicants argued, in the response to the first office action filed on July 16, 2004, regarding claims 1-28 being rejected under 35 U.S.C. §103 (a) as being unpatentable over Tello in view of Janacek that Tello discloses at column 2, lines 41-49 a method using portable e-mail addresses wherein a well-known address is translated to a literal address and returns the corresponding literal address value. Janacek discloses, at column 2, lines 57-64, a method for secure transmission of a message via a network wherein a recipient of the message is not a party to the network or maintains an active address within the network. Messages from a network-party sender addressed to an unknown user are deposited in a unique account created for the addresses recipient.

In response to the first office action claim 1 was been amended to include a limitation from claim 8 wherein the authenticity of an originator address associated with an outbound message is verified. This is done such that the authenticity of the originator address of the outbound message is verified to ensure that the outbound message has arrived from an originator computer system and/or username from which it purports to have arrived. This avoids a situation that allows a computer user to specify a fraudulent username as the originator of an email message (i.e., avoids false names in the FROM: field of an email message). Neither Tello nor Janacek, taken alone or in combination, disclose verifying the authenticity of an originator address associated with an outbound message.

With respect to the rejection of Claims 1-28 under 35 U.S.C. §103 (a) as being unpatentable over Tello et al. (U. S. Patent No. 6,381,634) in view of Barchi (U.S. Patent No. 6,507,866), Applicants argued that claim 1 has been amended to include a limitation from claim 8 wherein the authenticity of an originator address associated with an outbound message is verified. The Examiner stated, with respect to the rejection of claims 8 and 21, that Barchi discloses verifying the authenticity of an originator address associated with the outbound message at column 8, lines 1-50. Applicant respectfully disagrees with the Examiner's statement. A careful review of Barchi, and in particular column 8, lines 1-50, finds that Barchi discloses storing a field indicating the originator of a received e-mail message, and checking whether the number of received e-mails from the originator exceeds the threshold for the record. Barchi further discloses a user name and password required to log in to the system. Neither Tello nor Barchi disclose or suggest the verification of the originator address associated with an outbound message.

II. The Applicant's Position:

Claims 1-28

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter. Spamming is often done deliberately to use network resources. Email spamming may be combined with email spoofing, so that it is very difficult to determine the actual originating email address of the sender. Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. The specifying of a fraudulent username as the originator of an email message is known as "spoofing" an email address, and is done intentionally. Individuals, who are sending "junk" email or "SPAM", typically want the email to appear to be from an email address that may not exist. This way the email cannot be traced back to the originator.

These claims point out that the present invention, as part of controlling messages from an originator computer system, verification of the authenticity of an originator address associated with the outbound message is provided. The quota enforcement operation includes the steps of verifying an authenticity of an originator address associated with the outbound message. Using this technique, this embodiment of the invention can verify the authenticity of the originator address of the outbound message to ensure that the outbound message has arrived from an originator computer system and/or username from which it purports to have arrived. This avoids a situation that allows a computer user to specify a fraudulent username as the originator of an email message (i.e., "spoofing" an email address).

By way of the present invention, the verification of the authenticity of an originator address associated with the outbound message prevents email spoofing, since only messages with a "FROM" address that has been verified can be sent. Neither Tello nor Janacek nor Barchi disclose this verification of the authenticity of the originator address associated with an outbound message. Barchi's use of an account and a password does not prevent email spoofing, since it does not verify the authenticity of an originator address associated with an outbound message. In Barchi it is entirely possible that a user could validly login to the system and then send thousands of messages wherein the "FROM" field is spoofed with different addresses to avoid SPAM detection.

It is respectfully submitted, therefore, that the subject matter set forth in the claims of the present application is not anticipated by the arrangement of Tello, Janacek and Barchi.

(8) Claims Appendix

1. (Currently Amended) A method for controlling transmission of messages from an originator computer system, the method comprising the steps of:

detecting an outbound message from an originator computer system;

verifying an authenticity of an originator address associated with the outbound message;

performing a quota enforcement operation based on a message count and a message limit to produce a message transmission result; and

performing a selective transmit operation including at least one of:

i) transmitting the outbound message onto a computer network if the message transmission result contains a transmit value; and

ii) preventing transmission of the outbound message onto a computer network if the message transmission result contains a no-transmit value.

2. (Previously Presented) The method of claim 1 wherein the step of performing the quota enforcement operation includes the steps of:

comparing the message count associated with an originator identity of the outbound message with the message limit assigned to the originator identity of the outbound message to determine an occurrence of a message limit condition, and if the message limit condition occurs, setting the message transmission result to a no-transmit value, and if the message limit condition does not occur, setting the message transmission result to a transmit value; and

updating the message count associated with the originator identity of the outbound message.

3. (Original) The method of claim 2 wherein the step of comparing the message count associated with an originator identity of the outbound message includes the steps of:

obtaining an originator address associated with the outbound message;

obtaining the originator identity associated with the outbound message by performing an originator identity lookup based on the originator address; and

obtaining at least one message count associated with the originator identity by performing an message count lookup based on the originator identity.

4. (Original) The method of claim 3 wherein:

the step of obtaining an originator address includes retrieving a network address associated with the outbound message from a message connection establishment protocol used to transfer the outbound message from an originator computer system to a recipient computer system;

the step of obtaining the originator identity includes the step of querying a login database containing mappings of originator addresses to originator identities based on the originator address obtained in the step of obtaining an originator address; and

the step of obtaining a message count for the originator identity associated with the outbound message includes querying a quota database containing associations of message counts to originator identities based on the originator identity associated with the outbound message; and

wherein the message count is at least one message count that indicates, for an originator identity, a current number of outbound message transmitted over an elapsed time interval; and

wherein the message limit is at least one message limit corresponding to a respective at least one message count that indicates, for an originator identity, a maximum number of outbound messages that may be transmitted over a predetermine time interval.

5. (Original) The method of claim 2 wherein the step of updating the message count associated with the originator identity of the outbound message includes the steps of:

calculating a total number of recipients for the outbound message; and

incrementing the message count associated with the originator identity by the total number of recipients for the outbound message.

6. (Original) The method of claim 2 wherein:

the message limit indicates an amount of outbound messages that may be transmitted from the originator computer system over a certain period of time for the originator identity associated with the outbound message; and

wherein the originator identity of the outbound message is indicative of at least one of:

i) a specific user account operating under control of a computer user;

ii) a specific message sending user; and

iii) a specific domain.

7. (Original) The method of claim 2 wherein:

the message limit condition indicates if a computer user account associated with the originator identity used to transmit the outbound message is attempting to transmit a number of outbound messages that exceeds the message limit in a predetermined amount of time; and

wherein the message limit condition occurs if the step of comparing determines at least one of:

the message count exceeds the message limit; and

the message count is equal to the message limit.

8. (Currently Amended) The method of claim 2 wherein the quota enforcement operation includes the step of:

verifying authenticity of at least one recipient associated with outbound message.

9. (Original) The method of claim 1 wherein the step of performing a quota enforcement operation includes the step of:

comparing a previous message transmission result with a no-transmit value, and if the previous message transmission decision equals the no-transmit value, performing the step of performing a selective transmit operation.

10. (Original) The method of claim 1 wherein the step of detecting an outbound message includes the steps of:

searching a quota enforcement list for an originator address associated with the message, and if the originator address associated with the message is contained in the quota enforcement list, performing the steps of performing a quota enforcement operation and performing a selective transmit operation, and if the originator address associated with the message is not contained in the quota enforcement list, skipping the step of performing the

quota enforcement operation and performing the step of transmitting the outbound message from the computer system.

11. (Original) The method of claim 1 further including the steps of:

authenticating a connection from the originator computer system;

recording authentication information in a login database, the authentication information including an originator address assigned to the originator computer system and an originator identity associated with the originator address;

receiving, for transmission to a recipient computer system, the outbound message from the originator computer system;

forwarding the outbound message to a quota server to perform the steps of detecting an outbound message, performing a quota enforcement operation and performing a selective transmit operation.

12. (Currently Amended) A method for controlling transmission of messages onto a computer network, the method comprising the steps of:

detecting an outbound electronic mail message to be transmitted onto the computer network from an originator computer system and verifying an authenticity of an originator address associated with the outbound message;

in response to the step of detecting, comparing:

i) at least one message count associated with an originator identity associated with the outbound message;

to

ii) at least one message limit assigned to the originator identity associated with the outbound message that corresponds respectively to the at least one message count;

in order to determine a message transmission result that indicates if the originator computer system operating to transmit the outbound electronic mail message using the originator identity is attempting to transmit the outbound electronic mail message to a number of recipients that exceeds the message limit, and if the message transmission result is a no-transmit value, preventing transmission of outbound electronic mail messages onto the computer network for the originator identity, and if the message transmission result is a transmit value, allowing transmission of the outbound electronic mail message onto the computer network on behalf of the originator identity.

13. (Original) The method of claim 12, wherein:

the at least one message count includes a first message count and a second message count;

wherein the at least one message limit includes a first message limit and a second message limit;

wherein in the step of comparing, the first message count is compared to the first message limit to determine if the first message count exceeds the first message limit in which case the message transmission result is set to a no-transmit value; and

wherein in the step of comparing, the second message count is compared to the second message limit to determine if the second message count exceeds the second message limit in which case the message transmission result is set to a no-transmit value.

14. (Currently Amended) A computer system comprising:

a processor;

a memory system;

a network interface;

an interconnection mechanism coupling the processor, the memory system and the network interface;

wherein the memory system is encoded with a quota database and a quota server; and

wherein when the quota server performs on the processor in the computer system, the processor performing the quota system causes the computer system to control transmission of messages from an originator computer system onto a computer network by performing the operations of:

detecting an outbound message at the network interface wherein an authenticity of an originator address associated with the outbound message has been verified;

performing a quota enforcement operation for the outbound message based on a message count and a message limit obtained from the quota database in the memory system to produce a message transmission result; and

performing a selective transmit operation including at least one of:

i) transmitting the outbound message from the computer system if the message transmission result contains a transmit value; and

ii) preventing transmission of the outbound message from the computer system if the message transmission result contains a no-transmit value.

15. (Original) The computer system of claim 14 wherein when the processor performs the operation of performing the quota enforcement function, the processor causes the computer system to perform the operations of:

comparing the message count associated with an originator identity of the outbound message with the message limit assigned to the originator identity of the outbound message to determine an occurrence of a message limit condition, and if the message limit condition occurs, setting the message transmission result to a no-transmit value, and if the message limit condition does not occur, setting the message transmission result to a transmit value; and

updating the message count associated with the originator identity of the outbound message.

16. (Original) The computer system of claim 15 wherein when the processor performs the operation of comparing the message count associated with an originator identity of the outbound message, the processor causes the computer system to perform the operations of:

obtaining an originator address associated with the outbound message detected at the interface;

obtaining the originator identity associated with the outbound message by performing an originator identity lookup in a login database coupled to the computer system based on the originator address; and

obtaining at least one message count associated with the originator identity by performing an message count lookup in the quota database based on the originator identity.

17. (Original) The computer system of claim 16 wherein, when performed by the processor:

the operation of obtaining an originator address includes retrieving a network address associated with the outbound message from a message connection establishment protocol used to transfer the outbound message from an originator computer system to a recipient computer system;

the operation of obtaining the originator identity includes the querying a login database containing mappings of originator addresses to originator identities based on the originator address obtained in the operation of obtaining an originator address; and

the operation of obtaining a message count for the originator identity associated with the outbound message includes querying a quota database containing associations of message counts to originator identities based on the originator identity associated with the outbound message; and

wherein the message count is at least one message count that indicates, for an originator identity, a current number of outbound message transmitted over an elapsed time interval; and

wherein the message limit is at least one message limit corresponding to a respective at least one message count that indicates, for an originator identity, a maximum number of outbound messages that may be transmitted over a predetermine time interval.

18. (Original) The computer system of claim 15 wherein when the processor performs the operations of updating the message count associated with the originator identity of the outbound message, the processor further performs the operations of:

calculating a total number of recipients for the outbound message; and

incrementing the message count associated with the originator identity in the quota database by the total number of recipients for the outbound message.

19. (Original) The computer system of claim 15 wherein:

the message limit indicates an amount of outbound messages that may be transmitted from the originator computer system over a certain period of time for the originator identity associated with the outbound message; and

wherein the originator identity of the outbound message is indicative of at least one of:

i) a specific user account operating under control of a computer user;

ii) a specific message sending user; and

iii) a specific domain.

20. (Original) The computer system of claim 15 wherein:

the message limit condition indicates if a computer user account associated with the originator identity used to transmit the outbound message is attempting to transmit a number of outbound messages that exceeds the message limit in a predetermined amount of time; and

wherein the message limit condition occurs if the processor, when performing the operation of comparing, determines at least one of:

the message count exceeds the message limit; and

the message count is equal to the message limit.

21. (Currently Amended) The computer system of claim 15 wherein the when the processor performs the quota system to perform the quota enforcement operation, the processor performs the operation of:

verifying authenticity of at least one recipient associated with outbound message.

22. (Original) The computer system of claim 14 wherein the when the processor performs the quota system to perform the quota enforcement operation, the processor performs the operation of:

comparing a previous message transmission result with a no-transmit value, and if the previous message transmission decision equals the no-transmit value, the processor performs the selective transmit operation.

23. (Original) The computer system of claim 14 wherein when the processor performs the operation of detecting an outbound message, the processor further performs the operations of:

searching a quota enforcement list for an originator address associated with the message, and if the originator address associated with the message is contained in the quota enforcement list, performing the operations of performing a quota enforcement operation and performing a selective transmit operation, and if the originator address associated with the message is not contained in the quota enforcement list, skipping the operation of performing the quota enforcement operation and performing the operation of transmitting the outbound message from the computer system.

24. (Original) The computer system of claim 14 further including:

a remote access server coupled to the receive a connection from the originator computer system;

an authentication server coupled to the remote access server, the authentication server authenticating a connection from the originator computer system when the connection is received by the remote access server, the authentication server including a login extractor that records authentication information in a login database, the authentication information including an originator address assigned to the originator computer system and an originator identity associated with the originator address;

a port redirector coupled to the remote access server, the port redirector receiving, for transmission to a recipient computer system, the outbound message via the connection from the originator computer system and forwarding the outbound message to the interface for receipt by the quota server which, when performed on the processor, causes the processor to perform the operations of detecting an outbound message, performing a quota enforcement operation and performing a selective transmit operation.

25. (Original) The computer system of claim 24 wherein the port redirector is a data communications device capable of directing outbound messages based on content contained within the outbound message, and wherein when the port redirector receives an outbound message that is to be subject to message quota enforcement based upon content contained with the outbound message, the port redirector forwards the outbound message to the quota server.

26. (Currently Amended) A computer system for controlling transmission of messages onto a computer network, the computer system comprising:

a interface for detecting an outbound electronic mail message to be transmitted onto the computer network from an originator computer system wherein an authenticity of an originator address associated with the outbound message has been verified;

a quota server, the quota server comparing:

i) at least one message count associated with an originator identity associated with the outbound message;

to

ii) at least one message limit assigned to the originator identity associated with the outbound message that corresponds respectively to the at least one message count;

to determine a message transmission result that indicates if the originator computer system operating under the originator identity is attempting to transmit an outbound electronic mail message to a number of recipients that exceeds the message limit, and if the message transmission result is a no-transmit value, the quota server preventing transmission of outbound electronic mail messages onto the computer network for the originator identity, and if the message transmission result is a transmit value, the quota server allowing transmission of the outbound electronic mail message onto the computer network on behalf of the originator identity.

27. (Currently Amended) A computer program product having a computer-readable medium including computer program logic encoded thereon that when performed on a computer system, causes the computer system to control transmission of outbound messages onto a computer network, and wherein when the computer program logic is performed on a processor in the computer system, the computer program logic causes the processor to perform the operations of:

detecting an outbound message at the network interface;

verifying an authenticity of an originator address associated with the outbound message:

performing a quota enforcement operation for the outbound message based on a message count and a message limit obtained from the quota database in the memory system to produce a message transmission result; and

performing a selective transmit operation including at least one of:

i) transmitting the outbound message from the computer system if the message transmission result contains a transmit value; and

ii) preventing transmission of the outbound message from the computer system if the message transmission result contains a no-transmit value.

28. (Currently Amended) A computer program product having a computer-readable medium including computer program logic encoded thereon that when performed on a computer system, causes the computer system to control transmission of outbound messages onto a computer network, and wherein when the computer program logic is performed on a

processor in the computer system, the computer program logic causes the processor to perform the operations of:

detecting an outbound electronic mail message to be transmitted onto the computer network from an originator computer system and verifying an authenticity of an originator address associated with the outbound message;

in response to the step of detecting, comparing:

i) at least one message count associated with an originator identity associated with the outbound message;

to

ii) at least one message limit assigned to the originator identity associated with the outbound message that corresponds respectively to the at least one message count;

to determine a message transmission result that indicates if the originator computer system operating under the originator identity is attempting to transmit an outbound electronic mail message to a number of recipients that exceeds the message limit, and if the message transmission result is a no-transmit value, preventing transmission of outbound electronic mail messages onto the computer network for the originator identity, and if the message transmission result is a transmit value, allowing transmission of the outbound electronic mail message onto the computer network on behalf of the originator identity.

(9) Evidence Appendix

None

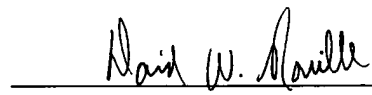
(10) Related proceedings appendix

None

Applicant hereby petitions for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

Respectfully submitted,

Date: February 9, 2006



David W. Rouille, Esq.
Attorney for Applicant(s)
Registration No.: 40,150
Chapin Intellectual Property Law, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661